DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on January 29, 2010 has been entered.

1. Claims 1-11 are currently pending consideration.

Response to Arguments

Applicant's arguments filed January 29, 2010 have been fully considered but they are not persuasive for the following reasons:

The Applicant argues that Hearn does not disclose a security device which houses an interface, storage, control system and a memory. This argument is not found persuasive. Hearn discloses a security device which houses a program memory (paragraph 0014), a storage (paragraph: 0016), a control system (paragraph 0013: a processing system), and an interface (paragraph 0015: connected in-line). Therefore, the Examiner asserts that Hearn does disclose a housing (Figure 1: item 35), which houses all the aforementioned elements.

In response to applicants' argument that the dedicated encryption device disclosed by Jackson must receive and authenticate a Crypto Variable or a Crypto

Variable and an Initialization Vector before accessing data to encrypt or decrypt and thus does not perform encryption and decryption on the fly. The examiner acknowledges that to enable the dedicated encryption device a Crypto Variable or a Crypto Variable and an Initialization Vector must be input to the dedicated encryption device. However, the examiner points out that the Crypto Variable or the Crypto Variable and the Initialization Vector are input once to enable the dedicated encryption device. After the dedicated encryption device has been enabled "any data read from the drive is automatically decrypted," and "all data written to the drive is automatically encrypted," without re-enabling the dedicated encryption device. See paragraphs 27-28 and 37-38. Accordingly, the dedicated encryption device is operable to encrypt data or decrypt data on the fly once the dedicated encryption device has been enabled.

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-10 are rejected under 35 U.S.C. 103(a) as being obvious over Hearn et al. (US 2005/0091522) in view of Jackson (EP 0911738 A2).

Regarding Claims 1, 6, and 8-9:

Hearn discloses a security device for protecting data (See figs. 1 and 2 ref. no. 35) having an interface ("ATA Cable" and "Bus Control and Interface Logic" See fig. 2 ref. nos. 33 and 43) for connection to a computing device ("CPU" See figs. 1 and 2 ref. no. 13), the security device is located in-line between the interface and the data storage ("Security Device" See figs. 1 and 2 ref. no. 35), a data storage ("Storage Device" See figs. 1 and 2 ref. no. 21), a control system ("Application Program" See paragraph 108), and a memory that includes program data executable on the computing device to perform user authentication ("Flash ROM" See fig. 2 ref. no. 41 and paragraphs 106-108), wherein the control system is configured to expose the memory to the interface to facilitate user authentication and at least until user authentication and to expose the data storage to the interface only upon successful user authentication ("The application program stored in flash ROM 41 for the security device 35 is generally designed to intercept and control the computer system's boot process and provide authentication by means of a login ID and password before access to the protected storage media is permitted." See paragraph 108).

Hearn does not disclose the security device includes an encryptor that is operable to encrypt on the fly data received from the interface and to forward the data once encrypted to the data storage and decrypt on the fly data received from the data storage and to forward the data one decrypted to the interface.

Jackson discloses a hard disk drive having a dedicated encryption device (See fig. 2 ref. no. 4) connected to the read/write means for encrypting data to be written onto the hard disk drive and decrypting data to be read from the hard disk drive (See paragraph 8).

It would have been obvious to one of ordinary skill in the art at the time of the invention to the security device disclosed by Heard to include a dedicated encryption device such as that taught by Jackson in order to remove the onus from the user to ensure that all files that should be protected by means of encryption are so protected (See Jackson paragraph 7).

Regarding Claim 2:

The above stated combination of Hearn and Jackson discloses the control system is configured to reboot the computing device after successful user authentication and before exposing the encryptor to the interface ("The operating system of the security device 37 then signals the authentication application program run by the host CPU 13 at 120 that the security device bus control and interface logic is configured to adopt the data access profile of the user, whereupon the application program at 121 issues the software interrupt vector to the host CPU13 invoking a warm boot. The appropriate soft boot vector is then loaded and the host CPU 13 causes a soft system re-start or warm boot at step 85." See Hearn paragraphs 143-145).

Regarding Claim 3:

The above stated combination of Hearn and Jackson discloses the memory has a portion of a memory storage system provided with one or more bootable programs ("The security device provides for a custom boot sector to be loaded into the RAM of the host CPU 13, which then executes an authentication application program requiring correct user authentication before allowing the computer system to proceed with its normal boot sector operation and operating system loading." See Hearn paragraph 125).

Regarding Claim 4:

Hearn discloses a security device for protecting data (See figs. 1 and 2 ref. no. 35) having a first interface ("ATA Cable" and "Bus Control and Interface Logic" See fig. 2 ref. nos. 33 and 43) for connection to a computing device ("CPU" See figs. 1 and 2 ref. no. 13), a second interface ("ATA Cable" and "Bus Control and Interface Logic" See fig. 2 ref. nos. 33 and 43) for connection to a data storage ("Storage Device" See figs. 1 and 2 ref. no. 21), the security device is located in-line between the interface and the data storage ("Security Device" See figs. 1 and 2 ref. no. 35), a control system ("Application Program" See paragraph 108), and a memory that includes program data executable on the computing device to perform user authentication ("Flash ROM" See fig. 2 ref. no. 41 and paragraphs 106-108), wherein the control system is configured to expose the memory to the interface to facilitate user authentication and at least until user authentication and to expose the data storage to the first interface only upon successful user authentication ("The application program stored in flash ROM 41 for the security device 35 is generally designed to intercept and control the computer system's boot process and provide authentication by means of a login ID and password before access to the protected storage media is permitted." See paragraph 108).

Hearn does not disclose the security device includes an encryptor that is operable to encrypt on the fly data received from the first interface and to forward the data once encrypted to the second interface and decrypt on the fly data received from the second interface and to forward the data one decrypted to the first interface.

Jackson discloses a hard disk drive having a dedicated encryption device (See fig. 2 ref. no. 4) connected to the read/write means for encrypting data to be written onto the hard disk drive and decrypting data to be read from the hard disk drive (See paragraph 8).

It would have been obvious to one of ordinary skill in the art at the time of the invention to the security device disclosed by Heard to include a dedicated encryption device such as that taught by Jackson in order to remove the onus from the user to ensure that all files that should be protected by means of encryption are so protected (See Jackson paragraph 7).

Regarding Claim 5:

The above stated combination of Hearn and Jackson discloses the control system is configured to reboot the computing device after successful user authentication and before exposing the encryptor to the interface ("The operating system of the security device 37 then signals the authentication application program run by the host CPU 13 at 120 that the security device bus control and interface logic is configured to adopt the data access profile of the user, whereupon the application program at 121 issues the software interrupt vector to the host CPU13 invoking a warm boot. The appropriate soft boot vector is then loaded and the host CPU 13 causes a soft system re-start or warm boot at step 85." See Hearn paragraphs 143-145).

Regarding Claim 7:

The above stated combination of Hearn and Jackson discloses the memory includes a bootable program configured to automatically load into the computing device when the device is connected to the computing device and the computing device is powered up ("The security device provides for a custom boot sector to be loaded into the RAM of the host CPU 13, which then executes an authentication application program requiring correct user authentication before allowing the computer system to proceed with its normal boot sector operation and operating system loading." See Hearn paragraph 125).

Regarding Claim 10:

The above stated combination of Hearn and Jackson discloses the security device is physically interposed inline with the ATA cable 33 between the ATA adapter provided on the device interface logic and the storage devices (See Hearn fig. 1 ref. no. 35 and paragraph 100). The above stated combination of Hearn and Jackson further discloses the security device 35 would similarly be interposed between the SCSI drive device and the interface logic (See Hearn paragraph 103).

The above stated combination of Hearn and Jackson does not explicitly disclose the security device is integrated with the computing device through the first interface. However, the examiner respectfully points out that making the security device integral with the computing device is a matter of obvious engineering choice. See *In re Larson, 340 F.2d 965, 968, 144 USPQ 347, 349 (CCPA 1965).*

Regarding claim 11:

Hearn discloses a data storage which is external to said housing (see Abstract: *wherein the security device is connected in-line with a CPU and a data storage*).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to KAVEH ABRISHAMKAR whose telephone number is (571)272-3786. The examiner can normally be reached on Monday thru Friday 8-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Korzuch can be reached on 571-272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Kaveh Abrishamkar/
Primary Examiner, Art Unit 2431

/K. A./
04/10/2010
Primary Examiner, Art Unit 2431